Content Notes

Presentation Notes

Have slide showing as attendees assemble.

Introduce yourself, giving a brief review of IS background and instructional experience.

NOTE: Be prepared to answer questions throughout the presentation. If attendees look as if they do not understand a given point, take time to explain.

Content Notes

Presentation Notes

Transition: Remember that Information Security has to occur in a context of physical security.


Security Technologies
Technology and products to:
Identify and authorize people
Monitor computer use
Protect you from Internet threats
Protect you from malicious code
Protect your data
Help manage information security
Page 3

Content Notes

Both identification and authentication are necessary components of Information Security.

Identification: Identifies the user to the system/network, usually based on a unique user name.

Authentication: Verifying that the user is who they say they are

Modes of Authentication:

- *Something you know:* Password, PIN
- *Something you have:* Card, Token, Key
- *Something you are:* Fingerprint, face, retina or iris pattern
- *Something you do:* Behavioral: Signature, Voice pattern, key stroke pattern

Stronger authentication uses more than one mode.

Presentation Notes

Expand on the differences between the two.

Explain that you will focus on methods of authentication.

Content Notes

There are several ways to authenticate.

Presentation Notes

Content Notes

Passwords and PINs:

- Most common means of authentication
- Can be effective if created, used, and managed properly
- Pros: Easy to use and integrated with most systems
- Cons: Can be forgotten, written down, divulged, guessed, and mismanaged; Can be intercepted and then used

Presentation Notes

Ask for a show of hands as to how many companies represented use passwords or PINs

Content Notes

Tokens:

- Electronic card or device that is either inserted into a reader or produces a number that the user enters into the system
- Provides two-factor authentication if a PIN or code is required to unlock the card or token
- Can be part of a strong challenge/response authentication
- Pros: Much harder to break than passwords
- Cons: Higher cost, Card/token can be stolen/coerced

Presentation Notes

Ask if any of the attendees have had experience with tokens and if there have been any problems.

Content Notes

Biometrics:

- Body part is scanned and compared with a stored value of an authorized user
  - "Enrollment" process is performed for each user
- Can provide both Identification and Authentication
  - Requires ability to be very unique for each user in order to do identification
- Fingerprint: Highly accurate and unique
- Facial: Less accurate and subject to environmental conditions
- Retina scan: Highly accurate, but expensive and obtrusive
- Iris Scan: Accurate, less obtrusive
- Pros: Non-forgeable, strong authentication
- Cons: More expensive (through costs have fallen), User acceptance issues

Presentation Notes

Give an example, showing how biometrics may or may not be appropriate for a small business.

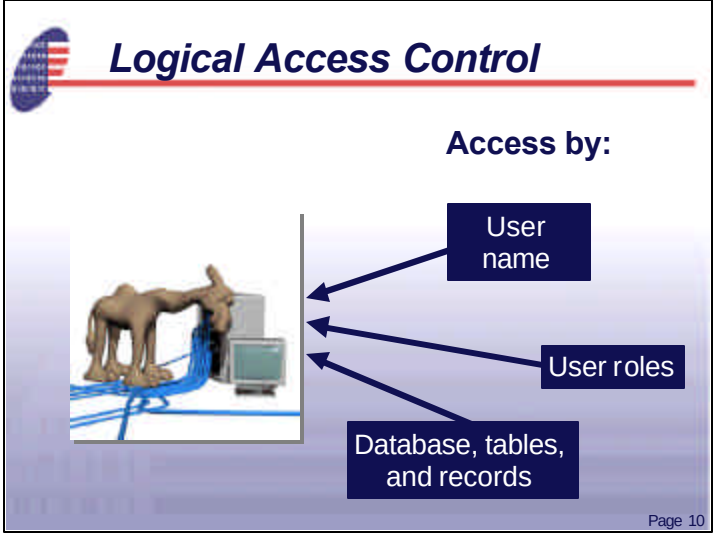
Give examples of how "strong authentication uses more than one mode."

Ways To Authenticate

Something you:

- Know
- Have
- Are
- **Do**

- Signature
- Voice pattern
- Key stroke pattern



Content Notes

Define file access by **user name**: Basic file access rights for users or groups of users:

- Read, Write/Delete, Execute
  - Beware of defaults to "everyone can read or write"
  - Requires good categorization of users and data
  - There is nothing to prevent someone from copying the data and giving it to other users
  - Effective only if set properly

Access by roles:

- System or software which defines access to data and operations by roles, rather than user names
- Each user joins or assumes a role when logging in

Database access control:

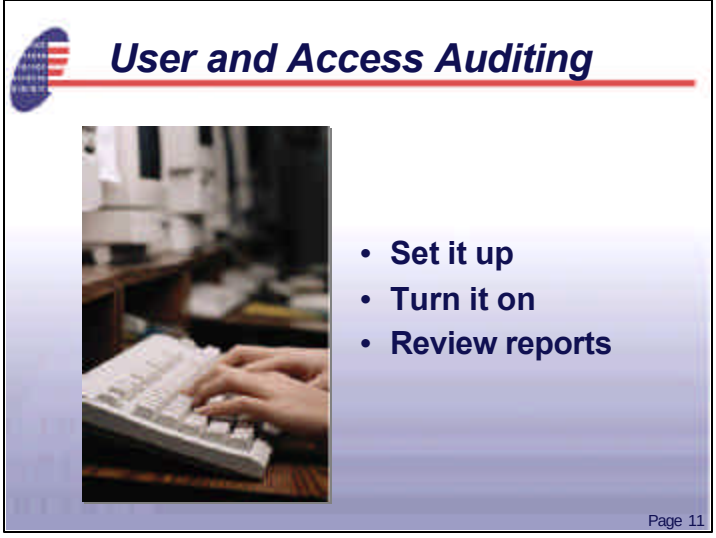
- Access rights assigned to database tables, or even records
- Beware of not tying database login with system login rights

Presentation Notes

Explain the dangers of the default to "everyone can read or write."

Give example of roles. (Accounting)

Give example of database access control.



Content Notes

Even if you implement identification and authentication procedures, you still need auditing.

OS, Database, Network components, and applications often already record:

- Login/logoff (success and failures) - user, time, device
- File accesses (success and failures)
- Use of privileges, change of privileges
- Administration changes
- Network access

You need to set it up, turn it on, and review the reports

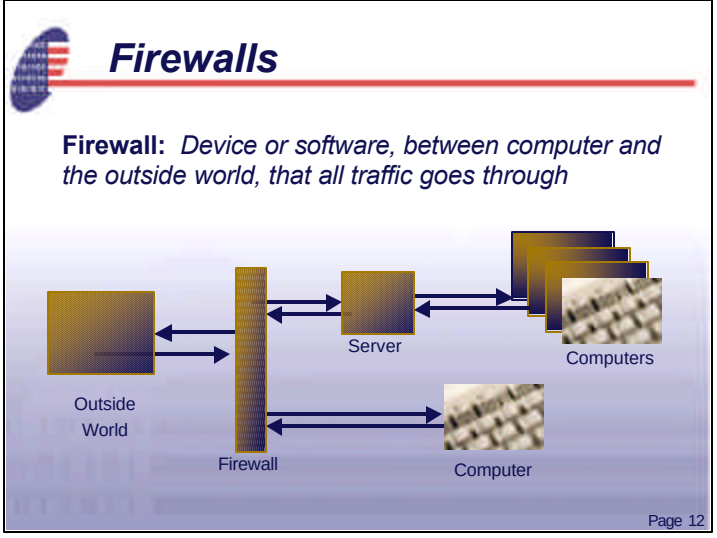
- Look at the failure events to see who's trying to do something they shouldn't be doing

NOTE: There may be legal constraints on whether and how much you can monitor people's actions.

Be sure employees understand the privacy guidelines affecting them.

Presentation Notes

Explain how they can find out how to access this information.



Content Notes

Firewall: Device or process that all traffic goes through between your computer(s) and the outside world

- Can ensure that only suitable connections and traffic goes back and forth
- Can prevent network-based attacks and probes through unused/unnecessary protocols, services, and ports
- Can restrict and monitor which computers can access the Internet
- Can restrict and monitor application data in and out of your network

Pros:

- A Firewall is today a required component for connection to the Internet
- Can protect internal machines which may not be secure

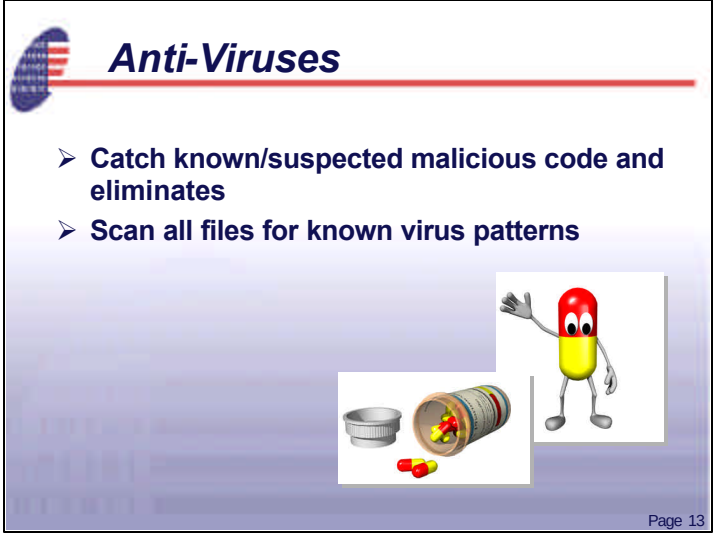
Cons:

- Cannot prevent bad things from happening on the internal network
- Performance may suffer; Single point of failure
- Cannot protect from vulnerabilities in the services allowed through the firewall

So, a firewall should not be your only solution for security!

Presentation Notes

Ask for a show of hands as to how many companies represented have a firewall. Mention that the term has become a buzzword for many computer users, though not many know what it really means.



Content Notes

Essential tool to catching any known (or suspected) malicious code on computers, and getting rid of them

Scans all files for known patterns which signify a virus

- Relies on a database of known viruses and other nasty programs
- Scans on file access, file creation/copy, and execution

Can also look for code characteristics which may indicate a new or mutated virus

Presentation Notes

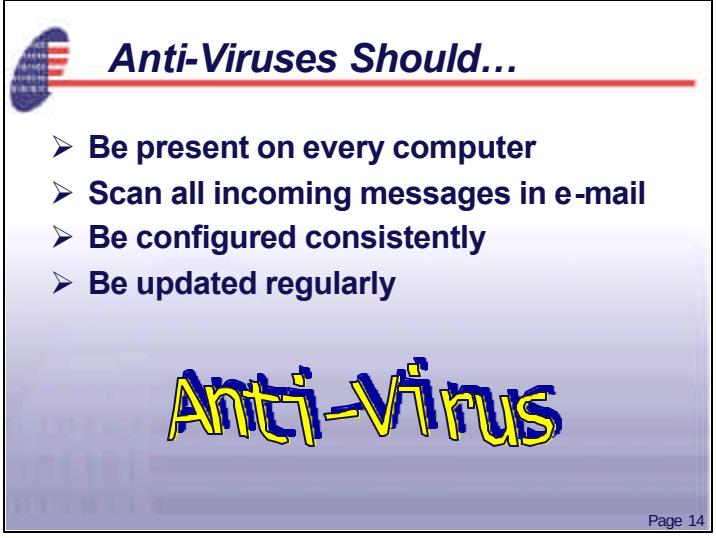
Ask how many currently have anti-virus programs at work or at home.

Ask how many have problems with staff who do not know how to use the anti-virus programs effectively.

Mention the names of the most popular.
Explain that most users interested in IS have firewalls and anti-virus programs, if nothing else.

Explain which type they should look for.

Emphasize the importance of AV as part of overall Information Security.



Content Notes

AV should be present on every computer, and should scan all incoming message on the mail server(s)

A company needs to have all AV copies configured consistently and updated regularly

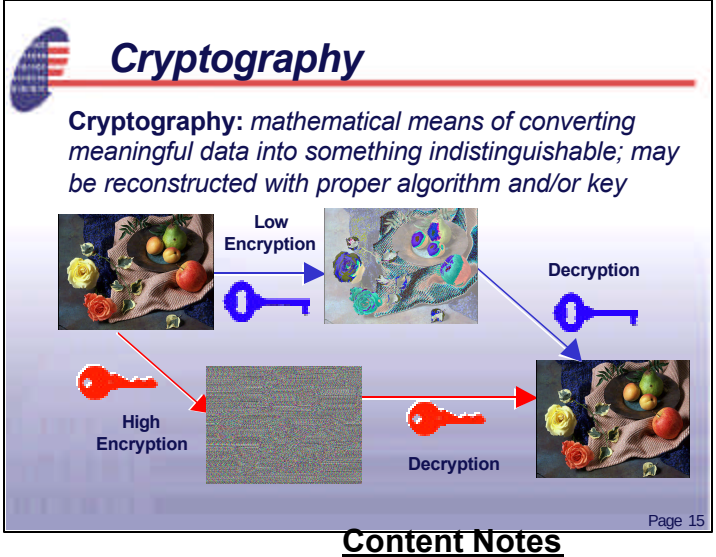
- Look for a "Enterprise" version that you can use on every computer, and manage from one central place

Pros: Essential element today for protection from malware

Cons: Often too relied upon for total security; Often updated "too late"

Use "auto update" feature

Presentation Notes



Content Notes

The strength of cryptography depends on two things:

•How good the algorithm is

•How long the key is (like a password)

- •128-bit is good
- •40-bit is not so good

"The best way to protect your information"

What can cryptography provide?

- •Data confidentiality – data cannot be viewed without the key
- •Data integrity – data cannot be modified without the key
- •Prevents fraud and misuse – only key holders can access data
- •Prevents forgery – data is effectively locked from re-creation
- •Non-repudiation – Only a key holder could have created the data you received

Symmetric Cryptography:

- A single key used to encrypt and decrypt
- It is generally a very fast process
- Security ultimately relies on the key's secure distribution

Asymmetric Cryptography:

- Two keys (one private, one public)
- Data is encrypted with public key, decrypted with private
- Much slower than symmetric cryptography (and longer keys)
- Private key encrypts your ID, public key decrypts it for source authentication (digital signature)

Look for cryptography products which are compliant with NIST FIPS 140-2

- Provides assurance for adherence to standards, technical goodness, and correct implementation

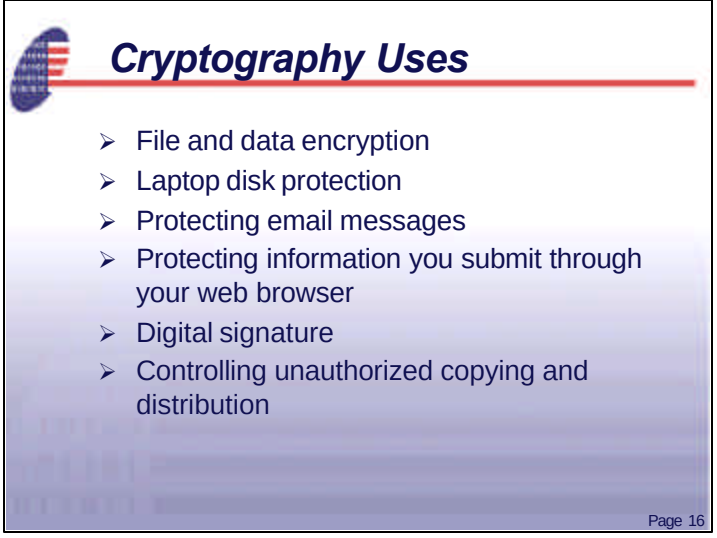
Certificate Authority: a trusted organization that only signs and distributes certificates for individuals or organizations that prove they are who they claim to be

User keys – private keys

Can be stored on client computer; Better if carried by user (smart card, token)

What can be encrypted?

- Files, email messages, passwords, network traffic, wireless data and voice transfer, identifying information, private information, programs, documents, …
  - Any information that you want to keep confidential and "locked"



Content Notes

PKI = CA + Management of keys + Applications

- The Certificate Authority Is a Trusted Organization that Only Signs and Distributes Certificates for Individuals or Organizations that Prove They Are Who They Claim to Be
- User's private key can be stored on client computer, and password protected
  - Better if key is carried by user (smart card, token)
- PKI Issues:
  - Interoperability with other organizations
    - Cross certification, cert. and algorithm compatibility
  - Key escrow: Backup of keys by other than the user
  - Certificate revocation: Applications need to check for it
- Subjects should be issued two pairs of private/public keys:
  - Encryption pair - private key is escrowed for backup
  - Signing pair - private key is not escrowed

Example of PK use: Secure Sockets Layer (SSL) Protocol Layer Between TCP/IP and HTTP(s), Telnet, FTP, et. al.

- Authenticates the Server to the Client Using PK Certificates
- Provides Protection Against Interception, Spoofing, Playback
- Can Also Authenticate the Client to the Server
- Protocol Handshake:
  - Client sends request to server to connect
  - Server sends signed certificate to client
    - Contains server's info, public key, certificate authority's name and signature (all encrypted with CA's private key)
  - Client verifies that CA is on its list and that this is an authentic certificate
  - Client then generates a session key and sends it to the server encrypted with the server's public key
  - Server uses its private key to decrypt session key
  - Session starts (encrypted/decrypted in both directions)

Several CA Certificates Are Hard-Wired into Netscape and Internet Explorer web browsers

Other CA Certificates Can be Downloaded if the User Is Willing to Accept Them

- For more details, see WWW.W3c.org or WWW.Netscape.com

Certificates Are Also Being Used to Authenticate Java Applets and ActiveX Code Source

Presentation Notes

Public Key (PK) Cryptography

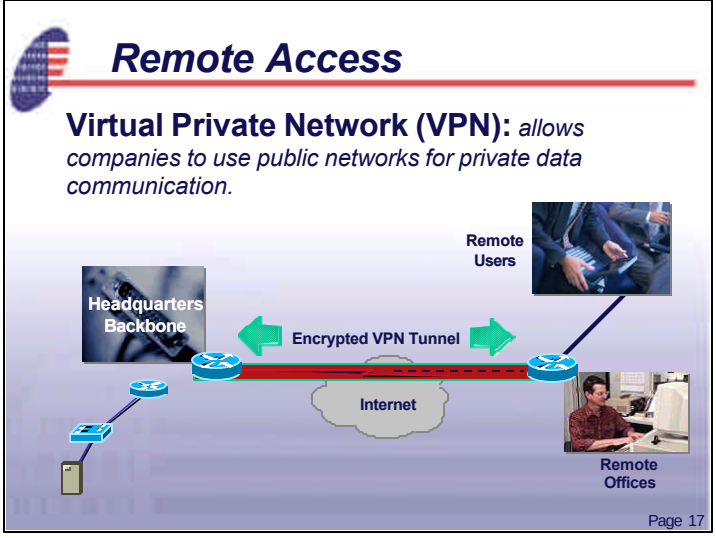
- Data/messages encrypted by owner/recipient's public key to provide confidentiality/integrity
- Data then only decrypted by owner/recipient's private key
- Owner/originator's identify plus data/message checksum is encrypted with private key (signed)
- Decryption by public key proves originator's identity and message integrity
- Entire process relies on validity of the public key

User identity, public key, and other information (Certificate) is created, signed, and issued by a mutually trusted third party - the Certificate Authority

Digital Certificate:

- Version
- Expiration Date
- Signature algorithm
- Public Key
- Signature

Issuer
Subject ID
Subject's



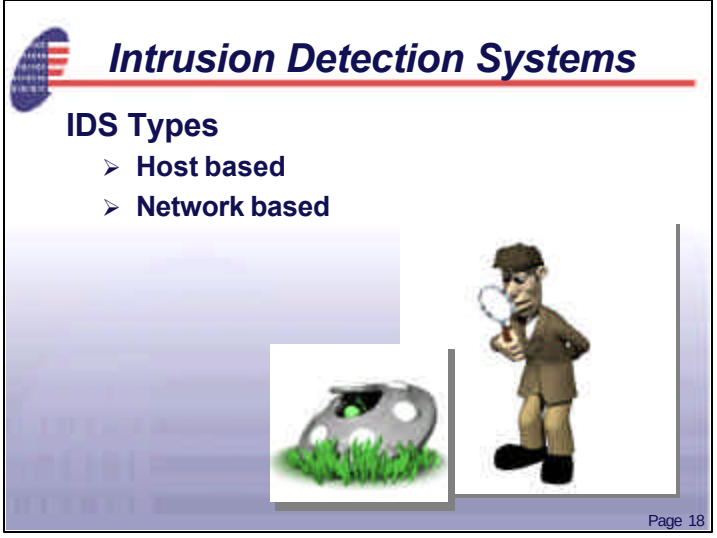
Content Notes

Can be used to authenticate and secure data transfer across the Internet

- Allows companies to use public networks for private data communication (i.e. establish an “Extranet”)

Free service is available through InfraGard.

Presentation Notes



Content Notes

Complete IDS products can consolidate information seen at multiple locations, and report to a central location of a problem.

Host Based:

- Can alarm on frequent failed or odd login attempts
- Can alert you of suspicious file access activity
- Can alert you about scans/attacks/probes from the network

Network Based

- Looks for known attack patterns (much like a virus checker)
- Can alert you of out-of-bounds or excessive network traffic

Often uses behavior monitoring to “learn” what is normal and what is not.

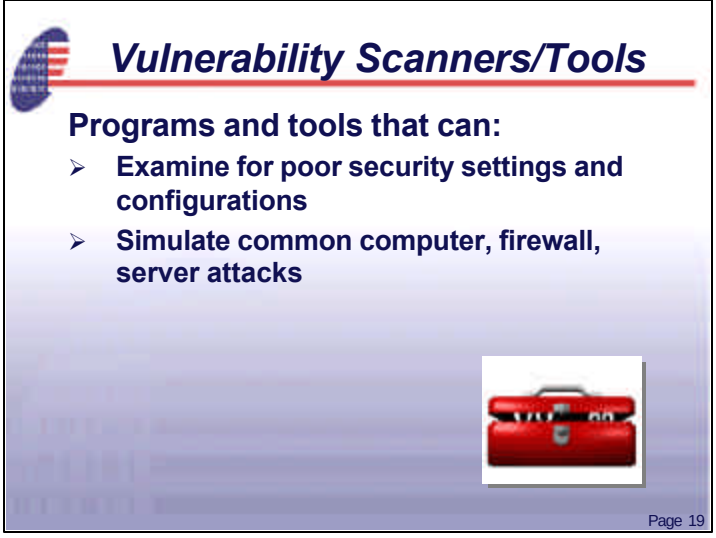
Pros:

- Effective in providing additional level of security by detecting attacks early and quickly
- Can detect outbound attacks by insider, in addition to attacks from the outside

Cons:

- Prone to False-Positives
- Can lull managers into thinking the network is protected (rather than only monitored)

Hardware/software which monitors the events or traffic on a computer or network to detect attacks and malicious behavior.



Content Notes

Programs and tools that can:

- Examine computer/network configuration for poor security settings and configurations
- Automatically try common attacks against your own computers, firewalls, servers, etc.

Presentation Notes

Content Notes

Types:

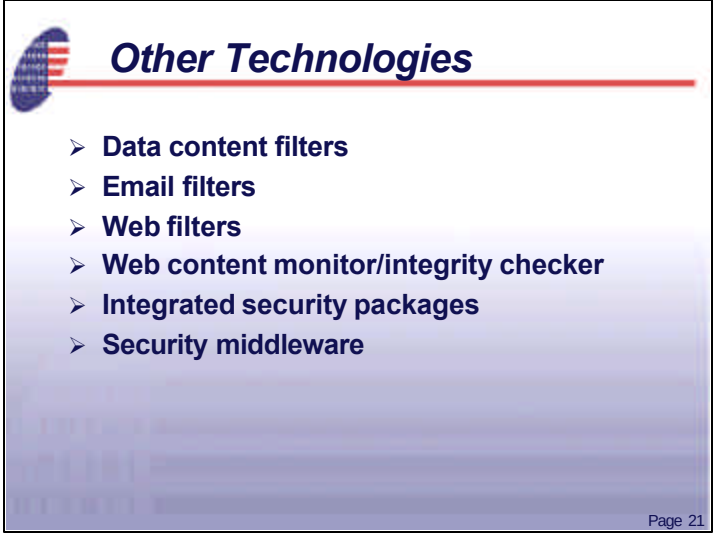
- Computer-based policy and patch checkers
- Password strength tools
- Network scanning
- Web-server scanning

•Pros:

- Can assist in finding the latest vulnerabilities

Cons:

- Provides only a snapshot of current problems (not how they got that way, or what will happen in the future)
- Therefore, if you use them, use them often and as part of an overall security process (to keep from getting in trouble in the first place)



Content Notes

Data content filters which examine inbound and outbound network data for:

- Proprietary information (based on keywords)
- Inappropriate language or subject

Email filters:

- Exist on mail server to scan outgoing (and maybe incoming) mail and attachments (similar to virus checking)

Web filters:

- Exist on firewall proxy to scan/disallow browsing to inappropriate web sites

Web content monitor / integrity checker

- Monitors web site and content for any changes
- May not prevent defacement, but will alert you to it quickly

Pros:

Can be effective education tool or deterrent of insider abuse

Cons:

Legal issues if not done correctly

Avoid conflict with expectations of privacy

Safer to use these to only collect statistics anonymously

Integrated security packages

- Single sign-on to integrate password mechanisms between OS, databases, network, and applications.

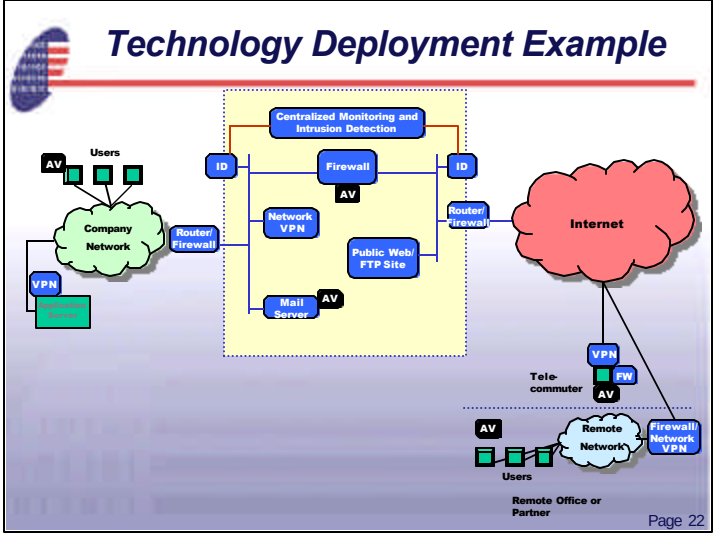
Security middleware:

- Data and files access control
- Account management

Presentation Notes

Explain why a small business might want to use these. Give examples of where they would be appropriate.

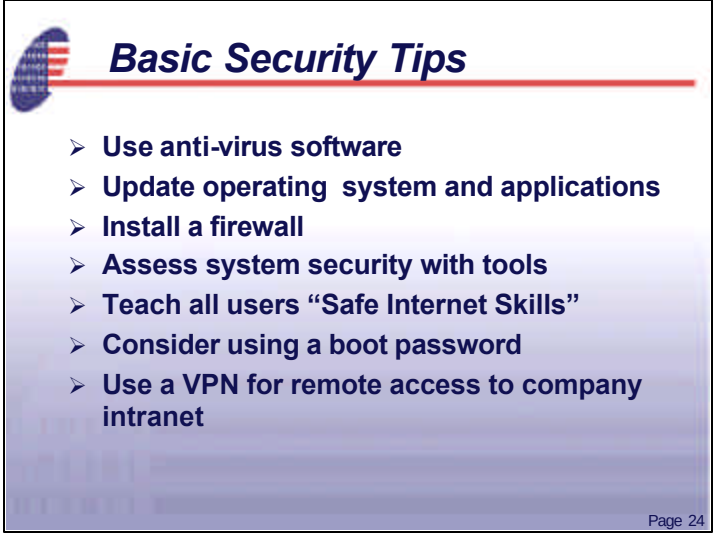
Explain that a business has to be specific in its requirements to implement:
•Integrated security package
•Security middleware


Technology Deployment Example
Centralized Monitoring and Intrusion Detection
Users
AV
ID
Firewall
AV
ID
Company Network
Router/ Firewall
Network VPN
Router/ Firewall
Internet
Public Web/ FTP Site
VPN
Mail Server
AV
VPN
FW
Tele-commuter
AV
AV
Remote Network
Firewall/ Network VPN
Users
Remote Office or Partner
Page 22

Reducing the Threats

Procedures, People, and Technology to address the threats…

	Information Theft	Denial of Service	Malicious Code
Internet Practices	◍		◍
Email Practices	◍		◍
Desktop Practices	◍		◍
Personnel Practices	◍		
Security Awareness	◍		◍
Physical Security	◍	◍	◍
Data backups		◍	◍
System updates/patches	◍	◍	◍
Identification & Authentication	◍	◍	
Logical Access Control	◍	◍	◍
Security Auditing	◍		
Firewalls	◍	◍	◍
Anti-Virus		◍	◍
Cryptography	◍		◍
Virtual Private Networks	◍	◍	
Intrusion Detection Systems	◍	◍	◍
Vulnerability Scanning	◍	◍	◍
Web/email/data filtering		◍	◍



Content Notes

Computer Security for the Home

Use Anti-Virus SW to detect/prevent Trojan horses and viruses

- Employers: Consider extending licenses to home use
- Get virus updates regularly!

Install a firewall

- Personal FW software (some good ones are free)
- Block file/printer sharing, all other unused services/ports

Run a tool which assesses your system's security

- Example: ShieldsUp® assessor at http://www.grc.com

Keep OS and applications updated and patched

- See vendor sites for tools, updates, and information

Teach everyone in the house the "Safe Internet Skills"

- Or get a separate computer for the risk takers

Consider the use of a power-on or "boot" password

Use a VPN for any remote access to company intranet

- Employers: Provide this for your employees!

Presentation Notes

Explain why information security is necessary for home computer use.

Explain what these are; refer to Presentation 1 as a good resource.

Explain how home computers may affect/be affected by networking with office computers.